

REMARKS

The Examiner has objected to Claims 51 and 53 due to informalities. Applicant has cancelled such claims, thus rendering the objections moot.

The Examiner has rejected Claim 29 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has clarified Claim 29 to avoid such rejection.

The Examiner has rejected Claims 1-57 under 35 U.S.C. 102(e) as being anticipated by FitzGerald, "Virus Bulletin", ISSN 0956-9979, October 1998. The Examiner has further rejected Claims 1-57 under 35 U.S.C. 102(e) as being anticipated by The Gale Group, "GeCAD introduces Romainian Antivirus 6.50", GUI Program News, v9, n12, Dec 1998. Still yet, the Examiner has rejected Claims 1-57 under 35 U.S.C. 102(e) as being anticipated by Hughes et al. (U.S. Patent No. 6,389,472).

Applicant respectfully disagrees with such rejection, especially in view of the amendments made to each of the independent claims. Specifically, applicant has amended each of the independent claims 1, 15, and 29 to substantially incorporate the subject matter of dependent Claims 2-5 et al.

With respect to dependent Claim 2 et al., presently incorporated into each of the independent claims, the Examiner has relied on the following excerpt from Hughes to make a prior art showing of applicant's claimed technique "wherein the monitoring step comprises the steps of: joining a channel; waiting a time delay; and leaving the channel."

"...chat room may be chosen and joined in any of a number of conventional ways." (Col. 16, lines 1-2)

Applicant respectfully asserts that the above excerpt from Hughes relates to joining a chat room for the purpose of creating a filter list (see Col. 15, lines 59-60).

Simply nowhere in Hughes is there any disclosure of joining a channel as one step in a plurality of steps for monitoring at least one channel..., in the context of applicant's claim language.

Furthermore, the Examiner has admitted that Hughes does not teach "waiting a time delay, and leaving the channel," and has also dismissed such claim language as being obvious. Specifically, the Examiner has stated that eventually the chat room would have to be left after a certain time period in order for the process to complete. Applicant respectfully disagrees with such an assertion. It would not be necessary to leave a chat room after a certain period of time in order to "[detect] a computer malware" in the manner claimed by applicant. Particularly, it would not be necessary to leave a chatroom in order to "[accept] data received from the monitored channel; and [store] and [log] the data received from the monitored channel" (see independent claims). Thus, applicant's claim language would not have been obvious, contrary to the Examiner's assertion.

The Examiner has also relied on Fitzgerald to make a prior art showing of applicant's claimed technique "wherein the monitoring step comprises the steps of: joining a channel; waiting a time delay; and leaving the channel" (Claim 2 et al.). Applicant notes that such reference merely discloses a 'bot' which monitors selected IRC channels. Applicant respectfully asserts that such general monitoring, as disclosed by Fitzgerald, does not rise to the level of specificity of applicant's claim language. In particular, simply nowhere in Fitzgerald is there even any mention of "joining a channel; waiting a time delay; and leaving the channel" (emphasis added), as specifically claimed by applicant.

In addition, the Examiner has relied on The Gale Group to make a prior art showing of applicant's claimed technique "wherein the monitoring step comprises the steps of: joining a channel; waiting a time delay; and leaving the channel" (Claim 2 et al.). Applicant notes that such reference merely teaches a "program designed to monitor Internet Relay Chat channels for Malware and Viruses." Again, applicant respectfully asserts that such general teaching of "monitor[ing]" does not rise to the level of

specificity of applicant's claim language, namely "joining a channel; waiting a time delay; and leaving the channel" (emphasis added).

Only applicant teaches and claims such a specific set of monitoring operations. As set forth on lines 9-13 of page 11 of the originally filed application, "IRC-aware" malwares typically use unsolicited so-called DCC Send requests to transmit themselves to a different computer on IRC. Sometimes, such requests are "triggered" whenever an unsuspecting user "leaves" a channel, etc. To this end, applicant's claimed invention more effectively monitors for these and/or other malwares.

With respect to dependent Claim 3 et al., presently incorporated into each of the independent claims, the Examiner has admitted that Hughes does not teach applicant's technique "wherein the monitoring step further comprises the step of: simulating user activities." Further, the Examiner fails to make any assertion as to why such claim language would be obvious in any way. Thus, applicant disagrees with such rejection and respectfully requests an allowance or a prior art showing of such specific claim language in the context claimed by applicant.

The Examiner has also relied on Fitzgerald and The Gale Group to make a prior art showing of applicant's claimed technique "wherein the monitoring step further comprises the step of: simulating user activities." However, after a careful review of such excerpts, applicant notes that simply nowhere in either reference is there even a suggestion of "simulating user activities," as claimed by applicant. For example, The Gale Group only generally teaches "a special program designed to monitor Internet Relay Chat channels," but fails to make any suggestion of monitoring that includes any sort of simulation of user activities. In addition, Fitzgerald even *teaches away* from applicant's specific claim language since it discloses that the 'bot' used for monitoring is "passive to avoid intrusions."

Only applicant teaches and claims such a specific, beneficial technique for use when monitoring. In particular, by simulating user activities, applicant's claimed

monitoring is more likely to trigger various malwares, and thus affords a more effective malware detection tool.

With respect to dependent Claim 4 et al., presently incorporated into each of the independent claims, the Examiner has again admitted that Hughes does not teach applicant's claimed technique "wherein the simulating step comprises the step of: transmitting a message to the channel." In rejecting such claim language, the Examiner has simply stated that it would have been obvious that the system transmit a message to the channel in order to join. Applicant respectfully disagrees. Specifically, Hughes even discloses that "the undesirable chat room...[is] joined to by entering its site address (e.g. its URL)" (see Col. 15, lines 64-67-emphasis added). Thus, since it is not necessary to join a chat room by transmitting a message, as is supported by Hughes, applicant asserts that such claim language would not have been obvious.

The Examiner has also relied on Fitzgerald and The Gale Group to make a prior art showing of applicant's claimed technique "wherein the simulating step comprises the step of: transmitting a message to the channel." For substantially the same reasons as argued with respect to Claim 3 et al., applicant respectfully asserts that neither reference even suggests applicant's specific claim language. Again, by simulating user activities via the transmission of a message to the channel, applicant's claimed monitoring is more likely to trigger various malwares, and thus affords a more effective malware detection tool.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by any of the references, especially in view of the amendments made hereinabove. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 58-67 below, which are added for full consideration:

“wherein transmitting the message to the channel is utilized for triggering the computer malware in the channel to be sent” (see Claim 58 and page 12, line 4 et al. of specification);

“wherein the storing and logging includes storing and logging a receipt time of the data and a sender of the data” (see Claim 59 and page 12, lines 8-9 et al. of specification);

“wherein an Internet Relay Chat client is utilized in the joining, the retrieving, and the monitoring” (see Claim 60 and page 15, lines 7-10 et al. of specification);

“wherein the Internet Relay Chat client automatically accepts and stores the data received from the monitored channel” (see Claim 61 and page 15, lines 14-16 et al. of specification);

“wherein the Internet Relay Chat client scans the received data to detect the computer malware” (see Claim 62 and page 15, lines 18-19);

“wherein the Internet Relay Chat client collects statistics” (see Claim 63 and page 15, lines 18-19 et al. of specification);

“wherein the Internet Relay Chat client notifies an administrator of the computer malware” (see Claim 64 and page 15, lines 19-20 et al. of specification);

“wherein the received data includes direct client-to-client DCC send requests” (see Claim 65 and page 17, line 14-15 et al. of specification);

“wherein the analyzing is automatically performed” (see Claim 66) (see page 18, lines 1-2 et al. of specification); and

“wherein the analyzing is performed manually” (see Claim 67 and page 18, lines 2-4 et al. of specification).

Thus, all of the independent claims 1, 15, and 29 are deemed allowable. Moreover, the remaining dependent claims 6-8, 20-22, 34-36, and 58-67 are further deemed allowable, in view of their dependence on such independent claims.

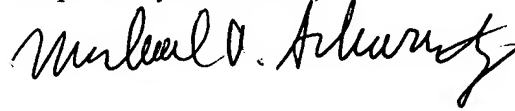
Additional Fees:

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with this application to Deposit Account No. 19-5127 (19903.0015).

Conclusion

In view of the foregoing, all of the Examiner's rejections to the claims are believed to be overcome. The Applicants respectfully request reconsideration and issuance of a Notice of Allowance for all the claims remaining in the application. Should the Examiner feel further communication would facilitate prosecution, he is urged to call the undersigned at the phone number provided below.

Respectfully Submitted,



Michael A. Schwartz
Reg. No. 40,161

Dated: August 31, 2005

Swidler Berlin, LLP
3000 K Street, N.W., Suite 300
Washington, D.C. 20007
(202) 424-7500